USAREUR COMPUTER-USER AGREEMENT

This appendix is a reference copy of the USAREUR Computer-User Agreement on the Regional Computer Emergency Response Team, Europe (RCERT-E) webpage at http://www.rcerte.5sigcmd.army.mil. Your systems administrator or information systems security officer will ask you to sign a copy of this agreement before issuing you a password.

**********

As a user of a USAREUR automated information system, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.

2. I will not import any software or install hardware on any computer (for example, client, workstation, server) without first getting written approval from my systems administrator (SA) or information systems security officer (ISSO).

3. I will not try to access data or use operating systems or programs, except as specifically authorized.

4. I know I will be issued a unique identifier and a password to authenticate my identifier (that is, a user ID). After receiving my user ID—

a. I will protect the password that authenticates the identifier.

b. If I am assigned an individual user account, I will not permit anyone else to use my password, nor will I will I reveal my password to anyone else. If my account is on a classified network, I will protect the password in accordance with the level of the network's classification level.

c. I am responsible for all activity that occurs on my individual account once my password has been used to log on.

d. If I have a classified account, I will change my password at once every 3 months.

e. If I have an unclassified account, I will change my password a least twice a year.

f. I will ensure that my passwords for both classified and unclassified accounts meet current USAREUR standards (for example, length, character set, no prohibited sequences or combinations) as directed by the ISSO.

g. I will not store my password on any processor or microcomputer or on any magnetic or electronic media unless approved in writing by the ISSO.

h. I will not tamper with my computer to avoid adhering to USAREUR password policy.

i. I will never leave my classified computer unattended while I am logged on or unprotected by a "passworded" screensaver.

5. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

6. I know that if connected to the Secure Data Network (SDN), my system operates at least in the U.S. Secret, "system-high" mode.

a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process).

b. I must protect all material printed out from the SDN at the system-high level until I or someone with the appropriate clearance personally reviews and classifies the material.

c. I will not enter information into a system if the information has a higher classification than the system. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the ISSO.

d. If connected to the SDN, only U.S.-cleared personnel are allowed unescorted access to the system.

e. Magnetic disks or diskettes will not be removed from the computer area without the approval of the local commander or head of the organization.

7. My site ISSO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the systems administrator or the ISSO.

8. I will check all magnetic media for malicious software before loading it onto a USAREUR system or network.

9. I will not forward chain-mail or virus warnings. (The Regional Computer Emergency Response Team, Europe, issues virus alerts and threat advisories.) I will report chain e-mail or virus warnings to my ISSO and delete the message. I will not attempt to run “sniffer” or other hacker-related software on the system.

10. I know I am subject to disciplinary action for any violation or abuse of access privileges.

11. If I observe anything that indicates inadequate security on the system I am using, I will immediately notify the site ISSO. I know what constitutes a security incident and know that I must immediately report such incidents to the ISSO.

12. I will comply with security guidance issued by my systems administrator and ISSO.

13 I understand that this agreement merely summarizes key points governing the use of Government computers in USAREUR, and is not an all-inclusive list of requirements and procedures governing the use of USAREUR computers.

PLEASE READ THE BELOW PARAGRAPHS: WHEN YOU SIGN THIS AGREEMENT YOU ARE IN FACT STATING THAT YOU FULLY UNDERSTAND THE OPSEC MESSAGE WHICH IS INSERTED.

Subj: (U) CHIEF OF STAFF OF THE ARMY OPSEC GUIDANCE (U//FOUO)
(U//FOUO) THE ENEMY IS ACTIVELY SEARCHING THE UNCLASSIFIED NETWORKS FOR INFORMATION, ESPECIALLY SENSITIVE PHOTOS, IN ORDER TO OBTAIN TARGETING DATA, WEAPONS SYSTEM VULNERABILITIES, AND TTPs FOR USE AGAINST THE COALITION. A MORE AGGRESSIVE ATTITUDE TOWARD PROTECTING FRIENDLY INFORMATION IS VITAL TO MISSION SUCCESS. THE ENEMY IS A PRO AT EXPLOITING OUR OPSEC VULNERABILITIES.

2. (U//FOUO) IT IS CRITICAL TO REMIND OUR PEOPLE THAT THE NEGLIGENT OR UNAUTHORIZED RELEASE OF SENSITIVE PHOTOS IS A SERIOUS THREAT TO OUR FORCES. LEADERS ARE ENCOURAGED TO:

2.A. (U//FOUO) REMIND ALL PERSONNEL THAT THE ENEMY WILL EXPLOIT SENSITIVE PHOTOS SHOWING THE RESULTS OF IED STRIKES, BATTLE SCENES, CASUALTIES, DESTROYED OR DAMAGED EQUIPMENT, AND ENEMY KIAs AS PROPAGANDA AND TERRORIST TRAINING TOOLS. FOR EXAMPLE, ANNOTATED PHOTOS OF AN ABRAMS TANK PENETRATED BY AN RPG ARE EASILY FOUND ON THE INTERNET. CAPTURED INSURGENT PAMPHLETS CONTAIN HAND DRAWINGS AND INSTRUCTIONS ON WHAT INSURGENTS BELIEVE ARE VULNERABLE PENETRATION POINTS ON TANKS, HMMWVS, BRADLEY FIGHTING VEHICLES, AND HELICOPTERS. RELEASING PHOTOS OUTSIDE OFFICIAL, PROTECTED CHANNELS MAY ALLOW THE ENEMY MATERIAL FOR HIS INFORMATION OPERATIONS AND TARGETING TTP AGAINST FRIENDLY FORCES. INSURGENTS ALSO USE WEBSITES TO COMMUNICATE, TRAIN, AND RECRUIT FOLLOWERS, OFTEN USING PHOTOS/VIDEO OF THEIR BATTLEFIELD SUCCESSES. WE CANNOT AFFORD TO HAVE OUR PHOTOS BECOME TRAINING AND RECRUITMENT TOOLS FOR THE ENEMY.

2.B. (U//FOUO) INFORM YOUR PERSONNEL THAT WE COULD UNWITTINGLY MAGNIFY ENEMY CAPABILITIES SIMPLY BY EXCHANGING PHOTOS WITH FRIENDS, RELATIVES, OR BY PUBLISHING THEM ON THE INTERNET OR OTHER MEDIA. WE ARE NOT LIMITING AUTHORIZED COMMUNICATION (TO INCLUDE THE APPROPRIATE USE OF PHOTOS) UNDER EXISTING PUBLIC AFFAIRS GUIDANCE, BUT WE MUST PROTECT PHOTOS THAT REVEAL TO THE ENEMY OUR BATTLE LOSSES, ONGOING FRIENDLY OPERATIONS, TTP, EQUIPMENT VULNERABILITIES, OR DISCLOSE INTELLIGENCE COLLECTION EFFORTS AND METHODS. MOREOVER, WE MUST PROTECT INFORMATION THAT MAY HAVE A NEGATIVE IMPACT ON FOREIGN RELATIONS WITH COALITION ALLIES OR WORLD OPINION.

3. (U//FOUO) OUR MISSION SUCCESS AND SOLDIERS LIVES DEPEND ON AGGRESSIVELY DENYING THE ENEMY ANY ADVANTAGE. I NEED YOUR FOCUS ON THIS CRITICAL ISSUE.

COMPUTER: _____ SECURITY _____
USER NAME OFFICER NAME

DATE _____ DATE_____